



CHILD PROTECT
PLATFORM

MULTI-TENANCY SCHOOL SAFETY PLATFORM

Child Protect Platform Overview

A detailed professional overview for school leaders, safeguarding teams, IT managers, implementation partners, and multi-school decision makers.

Secure safeguarding operations for schools and multi-site organizations.

Structured reporting, safeguarding case management, encrypted evidence handling, role-based access, audit logging, secure onboarding, multi-language readiness, and operational assurance in one controlled environment.

Structured reporting	Case management	Evidence preservation
Role-based access	Audit history	Operational assurance

www.childprotect.co

EXECUTIVE SUMMARY

A stronger operating system for child protection work.

Child Protect Platform is designed to help schools move safeguarding work out of scattered email, folders, and informal notes into a controlled workflow for reporting, case management, evidence preservation, access control, and oversight.

Purpose Support schools with clearer safeguarding workflows and safer record handling.	Core users Safeguarding leads, school leadership, IT administrators, and multi-school operators.	Main value Better structure, controlled access, evidence context, and accountability.
--	--	---

In one sentence

Child Protect helps schools turn safeguarding concerns into controlled, accountable workflows.

The platform supports structured reporting, case follow-up, evidence management, role-based access, audit history, and multi-school oversight while keeping urgent safeguarding matters inside official reporting routes.

Contents

01	Why the platform exists
02	Detailed platform positioning
03	Roles and administration
04	Safeguarding workflow
05	Evidence lifecycle and assurance
06	Trust and secure operations
07	Multi-school and localization
08	Implementation path
09	Training and pricing
10	Buyer guidance and next steps

WHY THE PLATFORM EXISTS

Safeguarding information needs structure, protection, and accountability.

Child protection work can begin with a concern, disclosure, online incident, behaviour pattern, parent message, or staff observation. The risk is not only missing a concern - it is also losing context, exposing sensitive data too widely, or failing to keep a clear record of follow-up action.

Email is not a case record

Safeguarding work often becomes fragmented across inboxes, attachments, chats, paper notes, and individual devices.

Shared drives lose context

A folder can store files, but it does not explain what was reported, who reviewed it, what changed, or what action was taken.

Generic ticketing is not enough

Child protection cases need restricted visibility, careful evidence handling, safeguarding-specific workflows, and governance.

Access needs to be intentional

Sensitive information should be visible only to users with the right safeguarding responsibility.

Leadership needs visibility

School leaders and group operators need oversight without unnecessary exposure of private case details.

Implementation must fit reality

Schools need a setup path that reflects actual roles, reporting routes, evidence types, and escalation policies.

The problem is operational, not just technical.

Schools need a reliable way to capture concerns, preserve evidence, control access, document follow-up, and support leadership oversight without turning sensitive safeguarding work into ordinary email or ticketing activity.

DETAILED PLATFORM POSITIONING

More than a form: a secure safeguarding operations platform.

The expanded platform brief positions Child Protect as a controlled environment for safeguarding governance, not just a public reporting form. It is designed to protect, preserve, control, verify, and prove the safeguarding process from end to end.

Secure intake Capture concerns through structured workflows so reports begin with the right context and a controlled record.	Controlled access Use role, tenant, and school scope so users see only what their responsibility requires.
Evidence preservation Keep sensitive materials connected to the correct case history, metadata, users, and audit trail.	Operational continuity Support backup verification, health checks, recovery planning, and file safety checks for platform resilience.

Strategic message

Child Protect replaces informal safeguarding administration with a secure, auditable, multilingual, and operationally controlled system designed around the sensitivity of child protection work.

ROLES AND ACCESS MODEL

Every user has a defined responsibility and a controlled scope.

Safeguarding work involves different duties. A staff reporter, safeguarding lead, investigator, school administrator, tenant administrator, platform administrator, and auditor should not all see or do the same things.

Platform Administrator Manages platform-level configuration, tenant creation, tenant status, platform controls, secure onboarding links, and high-level operational governance.	Tenant Administrator Manages an organization or school group, including schools, tenant-scoped users, activation status, reset links, and multi-school oversight.
School Administrator Manages school-level settings and users within assigned boundaries, without broad access to unrelated schools or tenants.	Safeguarding Lead Reviews, triages, manages, and tracks safeguarding concerns, case status, actions, follow-up, and appropriate escalation.
Investigator Works on assigned concerns or evidence, documents findings, records updates, and supports resolution within authorized scope.	Staff Reporter Submits concerns through structured reporting tools with limited access and no unnecessary visibility into wider case records.
Auditor Reviews permitted records, activity, and logs for assurance without receiving unnecessary operational control.	

ADMINISTRATION MODEL

Platform, tenant, and school controls are separated.

The administration design supports single schools, multi-school groups, education providers, foundations, and organizations that need central oversight with local boundaries.

Platform administration

Create tenants, assign tenant administrators, control tenant status, issue onboarding links, and review platform-level setup activity.

Tenant administration

Create schools, configure language and timezone settings, manage school-scoped users, assign roles, and operate across multiple schools under one tenant.

School-level administration

Manage local users and school activity while preserving boundaries between schools and preventing cross-school access.

- 1 Platform administrators create and control tenant setup at the highest level.
- 2 Tenant administrators operate inside their own organization and manage schools and users without platform-wide access.
- 3 School-level users remain scoped to their assigned school unless a role explicitly allows broader access.
- 4 Accounts can be enabled, disabled, locked, unlocked, and recovered through reset or onboarding links while preserving historical accountability.

WHAT CHILD PROTECT DOES

A secure operating layer for safeguarding workflows.

The platform is organized around practical safeguarding work: reporting, case review, evidence handling, user permissions, audit visibility, and multi-school governance.



Structured concern reporting

Move observations, disclosures, online incidents, parent concerns, and staff reports into a clearer reporting workflow.

Safeguarding case management

Keep case context, updates, actions, status changes, and follow-up decisions together in one controlled record.

Evidence preservation

Attach files, screenshots, notes, and supporting materials to the right case instead of scattering them across inboxes and folders.

Role-based access

Separate reporter, reviewer, safeguarding lead, administrator, leadership, and group oversight responsibilities.

CORE CAPABILITIES CONTINUED

Designed for the work schools actually need to do.

Child Protect is positioned as a platform for controlled safeguarding operations, not a generic storage location or ordinary helpdesk tool.

Audit-ready history Support accountability with a record of activity, changes, and follow-up decisions.	Multi-school oversight Support school-level control and group-level visibility without mixing sensitive records across campuses.
---	--

Security and governance Use controlled workflows, access boundaries, privacy-aware handling, and trust documentation to reduce operational risk.	Thai/English readiness Support international and Thailand-focused schools with bilingual public information and planned bilingual workflows.
--	--

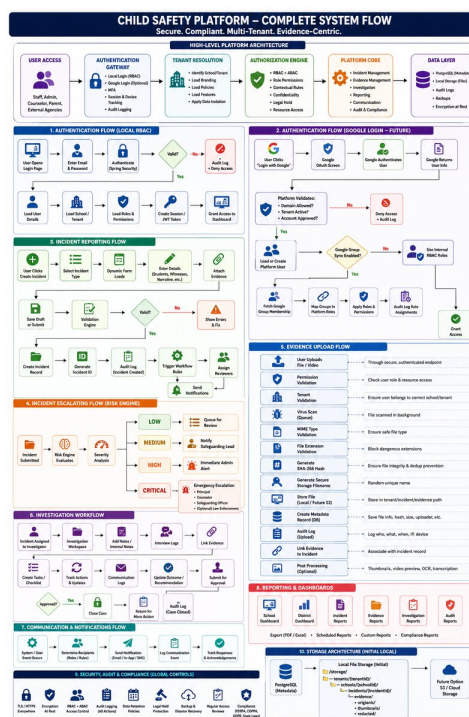
Report Capture concerns in a structured route.	Manage Keep case updates and actions together.	Preserve Link evidence to the right case context.	Oversee Support audit history and leadership visibility.
--	--	---	--

SAFEGUARDING WORKFLOW

From first concern to responsible follow-up.

The intended workflow helps a school move from informal communication to a repeatable safeguarding process with clearer accountability.

- 1 A concern is recorded through a structured reporting route instead of an informal message thread.
- 2 Safeguarding leads review, triage, and decide whether to create or update a case.
- 3 Case notes, actions, status changes, and follow-up decisions stay attached to the case record.
- 4 Evidence is uploaded or recorded in context and handled as part of the case workflow.
- 5 Role-based access limits who can view, update, administer, or oversee records.
- 6 Audit history and oversight views support accountability, review, and continuous improvement.



Platform workflow preview from the website flowcharts. Full flowchart assets are included on ChildProtect.co.

CASE MANAGEMENT

Turn safeguarding concerns into a controlled, accountable workflow.

A secure safeguarding case management platform for schools to record concerns, manage cases, preserve evidence, and control access.



Concern intake

Staff can report concerns through a structured workflow rather than relying on disconnected emails or informal notes.

Case lifecycle

Authorized users can review, triage, assign, update, and close or monitor cases based on the school workflow.

Action history

Notes, decisions, and follow-up actions stay connected to the case record for accountability.

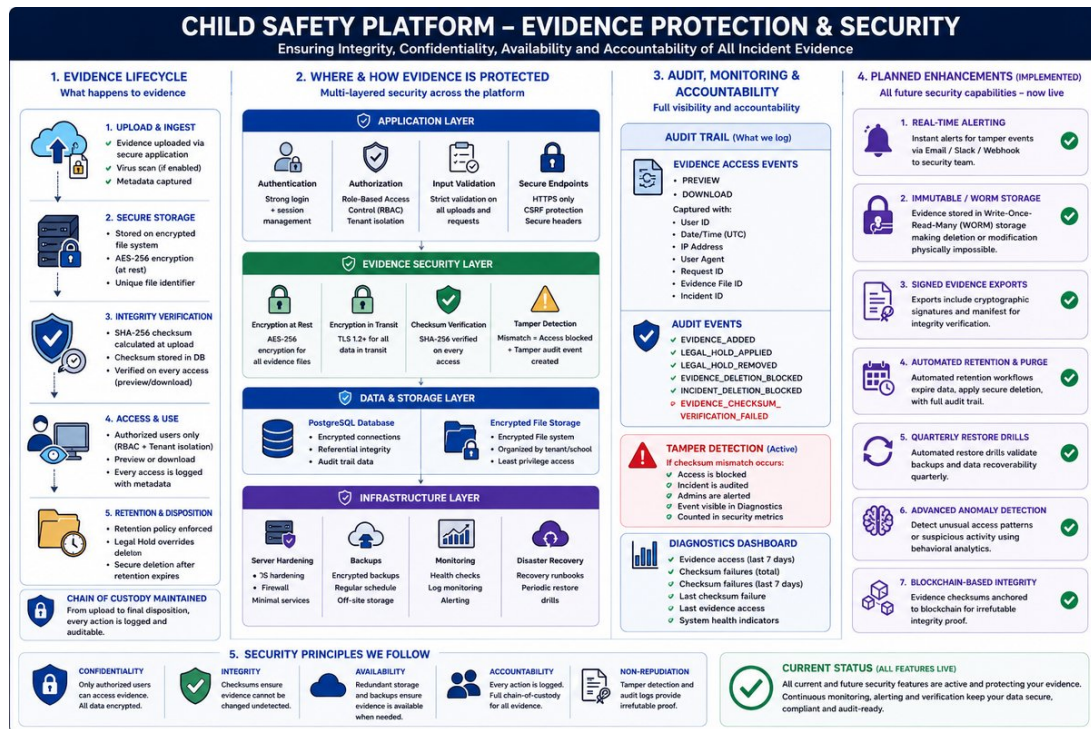
Leadership visibility

School leaders can understand workflow health and case activity without unnecessary exposure of sensitive details.

EVIDENCE PRESERVATION

Evidence is more than an attachment.

Safeguarding evidence can include screenshots, messages, documents, files, incident notes, or supporting context. The platform is designed to keep evidence linked to the right case and handled inside a controlled workflow.



Evidence upload and management flow preview.

Case-based organization

Evidence should remain connected to the relevant concern or case history.

Controlled visibility

Not every user should see evidence files or sensitive case details.

Context preservation

A file by itself is not enough; the platform helps preserve why it matters.

Reduced scatter

Move evidence away from personal devices, email attachments, and unmanaged shared folders.

EVIDENCE LIFECYCLE

Evidence is protected as a full lifecycle, not a casual upload.

The supplied platform brief emphasizes that evidence in safeguarding contexts may later support internal review, disciplinary action, regulatory reporting, law enforcement cooperation, or legal proceedings. That makes chain of handling and context critical.

Capture

Reports and supporting materials are captured through structured workflows rather than unmanaged email chains or shared folders.

Associate

Evidence stays linked to the correct tenant, school, report, case, user context, and timeline.

Protect

Encryption, authenticated application access, tenant/school scoping, and role-based permissions reduce exposure risk.

Scan

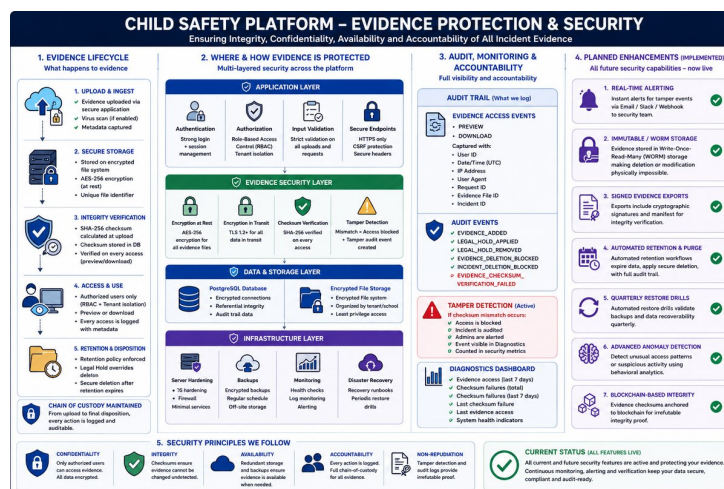
Uploaded files can be checked for malware or unsafe content before they are trusted in staff workflows.

Audit

Important evidence-related events such as upload, access, download, and administrative handling can be logged.

Recover

Backup verification and recovery planning help preserve sensitive records, files, metadata, and audit history over time.



Evidence upload and management flow preview from the website assets.

OPERATIONAL ASSURANCE

Security must keep working after launch.

The platform narrative goes beyond initial setup. It includes automation and operational readiness so administrators can trust that core protections, backups, scanning, and recovery processes remain credible.

Security boundary verification Automated checks can help confirm that users remain scoped to the correct tenant, school, role, and permission boundary.	Backup integrity Backups are only useful when they can be restored. Verification reduces the risk of silent backup failure.
Malware scanning Uploaded files can be scanned, flagged, or isolated before becoming broadly available inside safeguarding workflows.	Health monitoring Application, database, storage, email, scheduled jobs, evidence access, and critical workflows can be monitored for readiness.
Evidence integrity Checks can help verify that evidence remains accessible, linked to the correct record, and not silently lost or corrupted.	Disaster recovery readiness Operational recovery planning helps safeguard records remain available after infrastructure failure, cyber incidents, or operational mistakes.

Automation turns the platform from a passive repository into an actively monitored safeguarding environment.

Automated verification helps reduce silent failures across security boundaries, backup integrity, evidence availability, malware scanning, workflow readiness, and disaster recovery planning.

HARDENED HOSTING AND SECURE PROCESS FLOWS

The operating model limits public exposure and keeps internal services private.

The detailed security brief describes a hardened hosting approach in which public HTTPS access is separated from internal application and database services. This reduces exposed attack surface and supports operational confidence.

HTTPS reverse proxy Public traffic reaches nginx over HTTPS while internal application traffic is proxied behind the public web layer.	Local-only application service The application service is intended to listen locally rather than being directly exposed to the internet.
Local-only database PostgreSQL remains off public interfaces and communicates with the application internally.	Firewall default deny Only required public services should be allowed inbound; other services remain restricted.
SSH hardening Key-based access, limited authentication attempts, no root login, and monitoring reduce administrative exposure.	Security headers and monitoring Headers, logs, brute-force protection, and health checks support ongoing operational security.

- 1 External users connect over HTTPS to the public web endpoint.
- 2 nginx routes allowed application traffic internally through the reverse proxy layer.
- 3 The application communicates with PostgreSQL locally rather than exposing the database publicly.
- 4 Firewall rules, brute-force protection, logs, health checks, and audit records support monitoring and investigation.

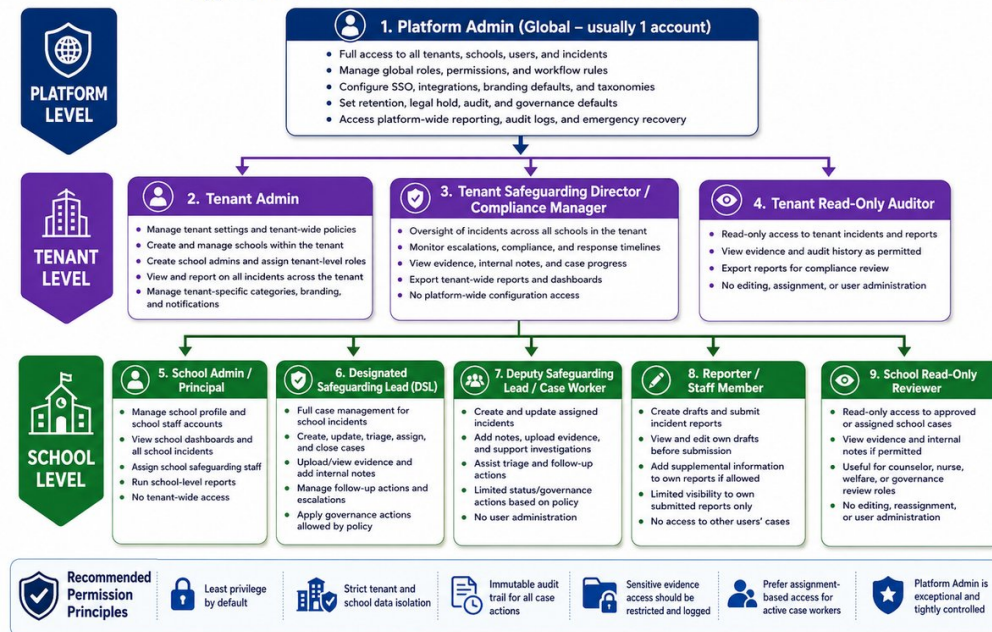
ACCESS CONTROL AND AUDIT HISTORY

Sensitive information should follow responsibility and role.

Child Protect emphasizes least-privilege access, data separation, and audit visibility so that safeguarding information is not overexposed.

Child Safety Platform – User Account Map & Suggested Permissions

Suggested RBAC structure: 1 platform admin, then tenant-level roles, then school-level roles



User account mapping and permissions preview.

Trust is a workflow feature.

For safeguarding software, trust is not only encryption or hosting. It includes who can see records, how evidence is handled, what activity is logged, and how leadership understands what happened.

SECURITY AND GOVERNANCE

Security, privacy, evidence, and governance in one place.

The Trust Center brings security, privacy, evidence handling, governance, and responsible data-handling information into one place for school decision makers.



Security overview

Explain how the platform approaches sensitive safeguarding records and controlled workflows.

Privacy and data handling

Support privacy-aware discussions for schools and education groups.

Evidence governance

Clarify why evidence should be handled inside a structured case workflow.

Responsible use

Reinforce that public forms and general email are not emergency reporting channels.

SECURE ONBOARDING AND USER LIFECYCLE

Accounts are created, activated, reviewed, and controlled intentionally.

The platform avoids unsafe manual password distribution by using onboarding and reset-link flows. Lifecycle controls matter because staff leave, responsibilities change, accounts can become risky, and historical records must remain accountable.

Controlled onboarding New users can receive a secure first-access or reset link instead of a password being shared manually.	Enable and disable Access can be removed when a staff member leaves or changes responsibility without deleting historical activity.
Lock and unlock Accounts can be locked when a security concern is identified and restored when appropriate.	Conflict prevention Duplicate email or username conflicts can be prevented during administration.
Scoped administration Tenant and school administrators manage users only inside their authorized boundary.	Audit history User creation, status changes, reset links, role changes, and administrative actions can be reviewable.

MULTI-SCHOOL OVERSIGHT

Safeguarding governance across every school without mixing sensitive data.

Support multi-school safeguarding oversight with controlled visibility, school separation, evidence preservation, and consistent case workflows.



Central standards Groups can promote consistent safeguarding workflows across schools or campuses.	Local control Each school can manage its own sensitive records and daily workflow.
Appropriate oversight Leadership can understand patterns and readiness without unnecessarily exposing case details.	Role separation Group, school, safeguarding, administration, and reporting roles can be handled separately.

THAILAND AND BILINGUAL READINESS

Designed to support PDPA-aware safeguarding operations in Thailand.

The website includes Thai and English information, Thailand-focused compliance positioning, and resources for schools that need bilingual communication and structured data handling.

Thai and English communication Public pages and resource content are available in both English and Thai.	PDPA-aware positioning The website emphasizes responsible data handling and privacy-aware safeguarding operations.
International school context Support for organizations that operate across languages, roles, and governance expectations.	Local reporting reminders Public resources reinforce that urgent concerns must follow official school and statutory reporting routes.

Use case Thai schools and international schools in Thailand.	Primary need Structured safeguarding workflows and careful data handling.	Important note The platform supports operations; it does not replace legal or emergency reporting obligations.
--	---	--

MULTI-LANGUAGE AND LOCALIZATION CAPABILITY

Usability improves when safeguarding workflows are understandable.

The platform is designed for supported interface languages such as English and Thai, with an extensible translation model for future languages. Localization improves adoption while preserving the same security, evidence, and audit boundaries.

Supported interface languages User-facing labels, navigation, messages, and workflow text can be displayed in supported languages.	Language switcher Users can operate in a familiar language where language switching is enabled.
Localized validation Translated messages and labels reduce reporting errors in sensitive workflows.	Tenant and school preferences Organizations and schools can be configured with language and regional preferences where appropriate.
Security consistency Changing language does not change role permissions, tenant isolation, evidence access, or audit behavior.	Regional readiness The platform can adapt to multilingual communities and international school environments.

IMPLEMENTATION PATH

A practical setup path for schools.

The best rollout starts with how the school actually works: who reports, who reviews, who manages cases, which evidence is handled, and what oversight is required.

1	Discovery and workflow review	Map who reports, who reviews, who manages cases, what evidence is handled, and what oversight is needed.
2	School and tenant setup	Configure the school, group, or campus structure, user boundaries, and administrative settings.
3	Role and permission mapping	Define reporters, safeguarding leads, case managers, administrators, leadership users, and group oversight roles.
4	Reporting and case forms	Align categories, fields, status labels, routing, evidence handling, and recordkeeping expectations.
5	Testing and launch readiness	Test permissions, reporting flows, case updates, evidence links, and audit visibility before launch.
6	Training and adoption support	Help staff understand what to report, where to report it, and why sensitive details need controlled workflows.



Administration and configuration overview preview.

WHO BENEFITS

A platform overview for leadership, safeguarding, and IT discussions.

Different teams evaluate safeguarding software through different lenses. This overview can support internal alignment before a demo.

Safeguarding leads Need structured reporting, follow-up, evidence context, and clear records of action.	School leadership Need confidence that concerns are recorded, reviewed, and managed responsibly.
IT and operations Need user roles, access control, implementation planning, and governance clarity.	Multi-school groups Need central oversight while preserving appropriate school-level separation.
International schools Need clear roles, bilingual readiness, and cross-functional safeguarding governance.	Parents and students Benefit indirectly from better school workflows and from related online safety training resources.

TRAINING AND AWARENESS

Age-appropriate online safety training for children, teens, parents, and schools.

The website includes online safety training positioning for students, parents, caregivers, and schools. Training content supports wider safeguarding awareness alongside the platform workflow.



Students

Age-appropriate digital safety awareness, safe sharing, privacy, gaming/chat risks, and reporting concerns.

Parents and caregivers

Warning signs, calm conversations, device routines, and response guidance when something feels wrong.

Schools

Awareness support that complements safeguarding policies, reporting procedures, and child protection workflows.

Training waitlist

The public website includes a waitlist for planned free online safety training and launch updates.

PRICING AND PACKAGES

Clear pricing for schools and multi-school organizations.

The website positions pricing around schools and multi-school organizations, with setup, monthly plans, multi-school options, and custom integrations.



School size and structure Pricing discussions depend on whether the deployment is for one school, several campuses, or a group.	Setup and onboarding Implementation planning includes configuration, roles, workflow alignment, and launch readiness.
Custom modifications Some schools may need custom workflows, integrations, or additional implementation support.	Demo before final scope A focused demo helps define which plan and rollout path best match the school context.

WHY DEDICATED SAFEGUARDING SOFTWARE

Email, shared drives, and ticketing tools were not built for child protection case records.

The website includes comparisons that explain why schools should avoid relying on generic tools for safeguarding evidence and case management.

Email Good for communication, weak as an authoritative safeguarding record.	Shared drives Good for storage, weak for chain-of-handling, context, permissions, and case status.
Ticketing tools Good for support queues, weak for safeguarding governance and sensitive case workflows.	Child Protect Designed around reporting, case follow-up, evidence context, role-based access, and audit history.

A child protection case is not an ordinary support ticket.

Safeguarding work requires careful boundaries, sensitive language, controlled evidence handling, and accountable follow-up. A purpose-built workflow helps reduce operational risk.

WEBSITE CONTENT MAP

What the current website covers.

The following map summarizes key English website pages used to build this platform overview. It can help teams decide what to read next.

Home	A stronger operating system for child protection work.
Schools	Safeguarding software for schools that need control, evidence preservation, and accountability.
Case management	Turn safeguarding concerns into a controlled, accountable workflow.
Evidence preservation	Protect safeguarding evidence from upload through review, retention, and recovery.
Trust Center	Security, privacy, evidence, and governance in one place.
Multi-school groups	Safeguarding governance across every school without mixing sensitive data.
Pricing	Clear pricing for schools and multi-school organizations.
Flowcharts	Platform flowcharts for sales, trust, and implementation clarity.
Buyer guide	Safeguarding Software Buyer Guide for Schools
Implementation checklist	Safeguarding Software Implementation Checklist

BUYER AND IMPLEMENTATION GUIDANCE

Useful questions before a demo.

The website includes buyer-guide and implementation-checklist resources. These questions help schools compare options and prepare for a realistic rollout.

Workflow fit Does the system reflect how safeguarding concerns are reported, triaged, escalated, and reviewed?	Permission model Can the school separate reporters, reviewers, case managers, administrators, and leadership oversight?
Evidence handling Can evidence be preserved with context, access control, and connection to the correct case?	Audit history Can authorized users see activity and changes over time?
Rollout readiness Are users, roles, reporting routes, and training needs clear before launch?	Governance alignment Does the system support local policy, school procedures, privacy expectations, and urgent reporting routes?

RECOMMENDED DEMO AGENDA

Make the demo specific to your school.

A focused Child Protect demo should be practical. The best discussions start with your safeguarding workflow and move into roles, evidence, oversight, and implementation.

- 1 Start with your current reporting routes and who receives safeguarding concerns.
- 2 Review how a concern becomes a case and how follow-up is documented.
- 3 Discuss how evidence is uploaded, protected, and connected to case history.
- 4 Map staff roles, permissions, school leadership visibility, and group-level oversight needs.
- 5 Talk through setup, onboarding, training, timeline, and bilingual requirements if relevant.
- 6 Confirm what should stay outside public forms and general email, especially active case details and urgent concerns.

Recommended next step

Use this overview to brief leadership, safeguarding, and IT colleagues. Then request a focused demo that uses your school structure and reporting workflow as the starting point.

- Website: www.childprotect.co/contact
- Email: inquiry@childprotect.co
- Ask about setup, pricing, onboarding, bilingual support, and custom workflow requirements.

IMPORTANT SAFETY NOTE

Do not submit urgent safeguarding incidents through public website forms or general email.

Public website forms and general email are not designed for active safeguarding case management. For urgent safeguarding matters, follow your school or organization's official safeguarding policy and reporting routes. If someone is in immediate danger, contact the appropriate emergency or statutory reporting service in your location.

Request a demo Use the website contact form to request a platform briefing.	Review trust information Start with the Trust Center if security or privacy is part of the evaluation.	Share internally Use this PDF and the overview PDF to brief leadership, safeguarding, and IT teams.
--	---	--



Child Protect Platform
Secure safeguarding software for schools and education groups
www.childprotect.co